Computer-Aided Reasoning for Software

Reasoning about Programs I

Emina Torlak

emina@cs.washington.edu

Overview

Last lecture

• Finite model finding for first-order logic with quantifiers, relations, and transitive closure

Today

- Reasoning about (partial) correctness of programs
 - Hoare Logic

A look ahead (LII-LI4)

Classic verification (LII, LI2, LI3)

 Checking that all (terminating) executions satisfy an FOL property on all inputs

Symbolic execution (14)

 Systematic checking of FOL properties of all executions of bounded length

A look ahead (LII-LI4)

Classic verification (LII, LI2, LI3)

 Checking that all (terminating) executions satisfy an FOL property on all inputs

Symbolic execution (14)

 Systematic checking of FOL properties of all executions of bounded length Active research topic for 45 years

Classic ideas every computer scientist should know

Understanding the ideas can help you become a better programmer

A bit of history

1967: Assigning Meaning to Programs (Floyd)

• 1978 Turing Award

1969: An Axiomatic Basis for Computer Programming (Hoare)

• 1980 Turing Award

1975: Guarded Commands, Nondeterminacy and Formal Derivation of Programs (Dijkstra)

• 1972 Turing Award







A tiny Imperative Programming Language (IMP)

Expression E

• $Z | V | E_1 + E_2 | E_1 * E_2$

Conditional C

• true | false | $E_1 = E_2 | E_1 \le E_2$

Statement S

- skip (Skip)
- **abort** (Abort)
- V := E (Assignment)
- S₁; S₂ (Composition)
- if C then S_1 else S_2 (lf)
- while C do S (While)

A minimalist programming language for demonstrating key features of Hoare logic.

Hoare triple

- S is a program statement (in IMP).
- P and Q are FOL formulas over program variables.
- P is called a *precondition* and Q is a *postcondition*.

Hoare triple

- S is a program statement (in IMP).
- P and Q are FOL formulas over program variables.
- P is called a *precondition* and Q is a *postcondition*.

Partial correctness (Hoare triple semantics)

• If S executes from a state satisfying P, and if its execution terminates, then the resulting state satisfies Q.

Hoare triple

- S is a program statement (in IMP).
- P and Q are FOL formulas over program variables.
- P is called a *precondition* and Q is a *postcondition*.

Partial correctness (Hoare triple semantics)

• If S executes from a state satisfying P, and if its execution terminates, then the resulting state satisfies Q.

Total correctness

• If S executes from a state satisfying P, then its execution terminates and the resulting state satisfies Q.

{**P**} S {**Q**}

[P] S [Q]

Hoare triple

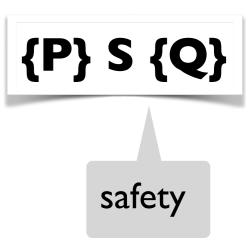
- S is a program statement (in IMP).
- P and Q are FOL formulas over program variables.
- P is called a *precondition* and Q is a *postcondition*.

Partial correctness (Hoare triple semantics)

• If S executes from a state satisfying P, and if its execution terminates, then the resulting state satisfies Q.

Total correctness

• If S executes from a state satisfying P, then its execution terminates and the resulting state satisfies Q.



[P] S [**Q**]

Hoare triple

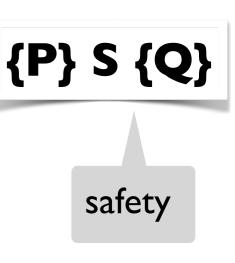
- S is a program statement (in IMP).
- P and Q are FOL formulas over program variables.
- P is called a *precondition* and Q is a *postcondition*.

Partial correctness (Hoare triple semantics)

• If S executes from a state satisfying P, and if its execution terminates, then the resulting state satisfies Q.

Total correctness

• If S executes from a state satisfying P, then its execution terminates and the resulting state satisfies Q.



liveness

[P] S [**Q**]

Hoare triple

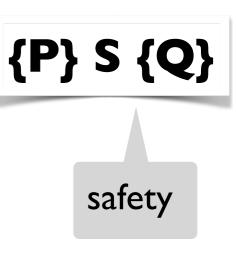
- S is a program statement (in IMP).
- P and Q are FOL formulas over program variables.
- P is called a *precondition* and Q is a *postcondition*.

Partial correctness (Hoare triple semantics)

• If S executes from a state satisfying P, and if its execution terminates, then the resulting state satisfies Q.

Total correctness

• If S executes from a state satisfying P, then its execution terminates and the resulting state satisfies Q.





{false} S {Q}

{false} S {Q}

• Valid for all S and Q.

{false} S {Q}

- Valid for all S and Q.
- {P} while (true) do skip {Q}

{false} S {Q}

• Valid for all S and Q.

{P} while (true) do skip {Q}

• Valid for all P and Q.

{false} S {Q}

• Valid for all S and Q.

{P} while (true) do skip {Q}

• Valid for all P and Q.

{true} S {**Q**}

{false} S {Q}

• Valid for all S and Q.

{P} while (true) do skip {Q}

• Valid for all P and Q.

{true} S {Q}

• If S terminates, the resulting state satisfies Q.

{false} S {Q}

• Valid for all S and Q.

{P} while (true) do skip {Q}

• Valid for all P and Q.

{true} S {Q}

• If S terminates, the resulting state satisfies Q.

{P} S {true}

{false} S {Q}

• Valid for all S and Q.

{P} while (true) do skip {Q}

• Valid for all P and Q.

{true} S {**Q**}

• If S terminates, the resulting state satisfies Q.

{P} S {true}

• Valid for all P and S.

Proving partial correctness in Hoare logic

Expression E

• $Z | V | E_1 + E_2 | E_1 * E_2$

Conditional C

• true | false | $E_1 = E_2 | E_1 \le E_2$

Statement S

- skip (Skip)
- **abort** (Abort)
- V := E (Assignment)
- S₁; S₂ (Composition)
- if C then S_1 else S_2 (lf)
- while C do S (While)

One inference rule for every statement in the language:

$$\begin{array}{l} \vdash \{P_1\}S_1\{Q_1\} \ \ldots \ \vdash \{P_n\}S_n\{Q_n\} \\ \vdash \{P\}S\{Q\} \end{array} \end{array}$$

If the Hoare triples $\{P_I\}$ S₁ $\{Q_I\}$... $\{P_n\}S_n\{Q_n\}$ are provable, then so is $\{P\}S\{Q\}$.

 \vdash {P} skip {P}

 $\vdash \{P\} \text{ skip } \{P\}$

⊢ {true} abort {false}

 \vdash {P} skip {P}

⊢ {true} abort {false}

 $\vdash \{Q[E/x]\} \times := E\{Q\}$

 \vdash {P} skip {P}

⊢ {true} **abort** {false}

 $\vdash \{Q[E/x]\} \times := E\{Q\}$

 $\begin{array}{c|c} \vdash \{P_I\} \ S \left\{Q_I\right\} & P \Rightarrow P_I & Q_I \Rightarrow Q \\ \\ \vdash \{P\} \ S \left\{Q\right\} \end{array} \end{array}$

 \vdash {P} skip {P}

 $\begin{array}{ll} \vdash \{P\} \ S_1 \ \{R\} & \vdash \{R\} \ S_2 \ \{Q\} \\ \\ \vdash \{P\} \ S_1; \ S_2 \ \{Q\} \end{array} \end{array}$

⊢ {true} **abort** {false}

 $\vdash \{Q[E/x]\} := E \{Q\}$

 $\vdash \{P_1\} S \{Q_1\} \quad P \Rightarrow P_1 \quad Q_1 \Rightarrow Q$ $\vdash \{P\} S \{Q\}$

 \vdash {P} skip {P}

 $\begin{array}{c} \vdash \{P\} \ S_1 \, \{R\} & \vdash \{R\} \ S_2 \, \{Q\} \\ \\ \vdash \{P\} \ S_1; \, S_2 \, \{Q\} \end{array} \end{array}$

⊢ {true} **abort** {false}

$\vdash \{P \land C\} \ S_1 \left\{Q\right\} \vdash \{P \land \neg C\} \ S_2 \left\{Q\right\}$

 \vdash {P} if C then S₁ else S₂ {Q}

 $\vdash \{Q[E/x]\} := E \{Q\}$

 $\vdash \{P_1\} S \{Q_1\} \quad P \Rightarrow P_1 \quad Q_1 \Rightarrow Q$ $\vdash \{P\} S \{Q\}$

 \vdash {P} skip {P}

 $\begin{array}{c} \vdash \{P\} \ S_1 \, \{R\} & \vdash \{R\} \ S_2 \, \{Q\} \\ \\ \vdash \{P\} \ S_1; S_2 \, \{Q\} \end{array} \end{array}$

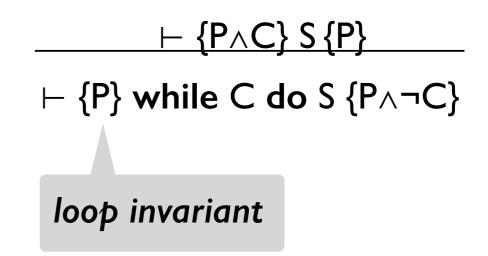
⊢ {true} **abort** {false}

 $\vdash \{P \land C\} S_1 \{Q\} \vdash \{P \land \neg C\} S_2 \{Q\}$

 \vdash {P} if C then S₁ else S₂ {Q}

 $\vdash \{Q[E/x]\} := E \{Q\}$

 $\begin{array}{c|c} \vdash \{P_I\} \ S \left\{Q_I\right\} & P \Rightarrow P_I & Q_I \Rightarrow Q \\ \\ \vdash \{P\} \ S \left\{Q\right\} \end{array}$



Example: proof outline

```
\{x \le n\}
while (x < n) do
  \{\mathbf{x} \le \mathbf{n} \land \mathbf{x} \le \mathbf{n}\}\
  \{x+l \le n\}
  x := x + |
  \{x \le n\}
\{x \le n \land x \ge n\} \qquad // \text{ while}
{x = n}
```

// consequence

// assignment // consequence

Example: proof outline with auxiliary variables

$$\{x = A \land y = B\}$$
$$\{y = B \land x = A\}$$
$$t := x$$
$$\{y = B \land t = A\}$$
$$x := y$$
$$\{x = B \land t = A\}$$
$$y := t$$
$$\{x = B \land y = A\}$$

Soundness and relative completeness

Proof rules for Hoare logic are sound

 $\mathsf{If} \vdash \{\mathsf{P}\} \mathsf{S} \{\mathsf{Q}\} \mathsf{then} \vDash \{\mathsf{P}\} \mathsf{S} \{\mathsf{Q}\}$

Proof rules for Hoare logic are relatively complete

If \models {P} S {Q} then \vdash {P} S {Q}, assuming an oracle for deciding implications

Summary

Today

- Reasoning about partial correctness of programs
 - Hoare Logic

Next lecture

Automating Hoare Logic with VC generation